|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | |  |
|  | | |
|  | | |
| 方圆ok1 | | | |
|  | **HUAWEI eSight**  Product Technical White Paper | | 附件1-16K |
|  | |
| **Issue** | **01** |
| **Date** | **2016-05-30** |
|  | |
| HUAWEI TECHNOLOGIES CO., LTD. | |
|  | | |

|  |
| --- |
| Copyright © Huawei Technologies Co., Ltd. 2016. All rights reserved.  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  Trademarks and Permissions  附件3-图 and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  Notice  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | [http://e.huawei.com](http://enterprise.huawei.com) |

Contents

[1 Executive Summary 1](#_Toc450834802)

[2 Overview 2](#_Toc450834803)

[3 Solutions 4](#_Toc450834804)

[3.1 eSight System 4](#_Toc450834805)

[3.1.1 Key Technologies 4](#_Toc450834806)

[3.2 Unified Monitoring, Diagnosis, and Troubleshooting 9](#_Toc450834807)

[3.2.1 Performance Collection and Prediction Analysis 10](#_Toc450834808)

[3.2.1.1 Introduction 10](#_Toc450834809)

[3.2.1.2 Key Technologies 11](#_Toc450834810)

[3.2.1.3 Function Constraints 11](#_Toc450834811)

[3.2.1.4 Typical Applications 12](#_Toc450834812)

[3.2.2 Alarm Information Collection and Notification 12](#_Toc450834813)

[3.2.2.1 Introduction 12](#_Toc450834814)

[3.2.2.2 Key Technologies 13](#_Toc450834815)

[3.2.2.3 Function Constraints 14](#_Toc450834816)

[3.2.2.4 Typical Applications 15](#_Toc450834817)

[3.2.3 Network Fault Diagnosis (Telepresence Conference) 15](#_Toc450834818)

[3.2.3.1 Introduction 15](#_Toc450834819)

[3.2.3.2 Key Technologies 15](#_Toc450834820)

[3.2.3.3 Function Constraints 16](#_Toc450834821)

[3.2.3.4 Typical Applications 16](#_Toc450834822)

[3.2.4 Rapid Configuration Backup and Restoration 18](#_Toc450834823)

[3.2.4.1 Introduction 18](#_Toc450834824)

[3.2.4.2 Key Technologies 18](#_Toc450834825)

[3.2.4.3 Function Constraints 19](#_Toc450834826)

[3.2.4.4 Typical Applications 19](#_Toc450834827)

[3.3 Security Management 19](#_Toc450834828)

[4 Conclusion 21](#_Toc450834829)

[5 Acronyms and Abbreviations 22](#_Toc450834830)

# Executive Summary

Huawei eSight network management system (NMS) is an integrated O&M management solution that is applicable to enterprise data centers, campus/branch networks, unified communications (UC), videoconferencing services, and video surveillance. eSight supports automatic deployment, visualized fault diagnosis, and intelligent capacity analysis of ICT devices (including servers, storage, eIMS, video surveillance, and UC devices, virtualization, switches, routers, WLAN, firewalls, telepresence systems, eLTE eNodeB, core network, terminals, equipment room facilities, and application software). eSight is mainly applied to scenarios such as the convergent O&M of data centers, intelligent O&M of Safe City projects, and WLAN full-life cycle management. eSight enables enterprises to enhance O&M efficiency and resource utilization, lower O&M costs, and ensure ICT system stability.

# Overview

With the explosive growth of enterprise ICT applications and in-depth construction of ICT systems, the ICT systems have been increasingly complex. A large number of ICT devices (including videoconferencing devices, IP phones, and video surveillance devices) as well as new technologies (such as cloud computing and bring-your-own-device) have been broadly applied in enterprise production and office systems, playing an inevitable role in enterprise operation.

As a result, enterprises have numerous network devices, storage devices, servers, and service systems from different vendors, difficult for IT administrators to perform efficient management. Service interruptions arising from device faults have severely influenced the normal operation of enterprise services. IT departments are responsible to ensure the stability and reliability of ICT systems, making ICT O&M a key part of ICT-led construction.

Diversified enterprise ICT services require refined ICT management. How to effectuate unified network-wide device management? How to quickly generate warning, detect problems, and rectify problems? Enterprises demand a unified and efficient system to manage devices. Huawei eSight system helps enterprises implement ordered O&M while reducing labor, time, and investment costs.

In response to customer requirements, the eSight system supports unified maintenance and management over a diversity of network, voice, and video surveillance terminals, and provides a diversity of service components for customers to build their own operation and maintenance environments based on a flexible combination of the service components.

To serve enterprise customers with different needs, eSight system is classified into Compact, Standard, and Professional editions, as described in the following table.

|  |  |
| --- | --- |
| Edition | Function |
| eSight Standard | * alarm management, performance management, topology management, configuration file management, network element (NE) management, link management, log management, physical resources, electronic label, IP topology, smart configuration tool, custom device management, security management, terminal access management, MIB management, VLAN management and AR voice management. * System monitoring tool, database backup/restoration tool. * Device management (UC, telepresence, video surveillance, storage, server, host, FusionAccess, FusionCompute and eLTE terminal). * Service management: OpenSDK management, smart report, storage report, WLAN management, MPLS VPN management, MPLS VPN tunnel management, SLA management, network traffic analyzer (NTA), security policy management (Secure Center), IPSec VPN management, server stateless computing management, server deployment management and infrastructure management. |
| eSight Professional | In addition to the functions in the Standard edition, the Professional edition also offers the following functions:   * Hierarchical network management * The Linux two-node cluster system supports two-node cluster hot standby. |

# Solutions

## eSight System

Operation and maintenance personnel of enterprises usually face a rather complicated network and varied services. They need to operate among multiple management systems to monitor services and locate faults, which is time-consuming and inconvenient. Therefore, to improve the operation and maintenance efficiency, a unified management system is required to provide centralized monitoring, one-stop service provisioning, and intelligent fault location.

To meet customer requirements, the eSight system leverages component-based and web-based technologies, network-wide status monitoring and troubleshooting (unified alarm and performance management), as well as rich optional service components to help users build a most appropriate and ease-of-use O&M environment. A single set of management software helps users easily manage the entire network.

### Key Technologies

1. Component-based Management to Customize O&M Platforms

eSight offers diverse service components that leverage the OSGi framework to support dynamic plug-and-play capabilities. Users can purchase and deploy most appropriate service components based on their demands.

eSight manages all service components through a unified web portal. Using the JMS-based communication bus, service components can share data and cooperate with each other to provide cross-system and cross-service value-added functions.

Advantages:

* Unified platform, consistent style, and optimal user experience.
* On-demand and flexible customization, reducing costs and avoiding duplicate investments.

eSight architecture



The following table lists optional service components and their functions.

|  |  |  |
| --- | --- | --- |
| Type | Component | Description |
| Management platform | eSight Platform | Offers basic network management functions, such as resource, topology, fault, and performance management. |
| Device management components | eSight Network Device Manager | Offers basic management and configuration over network devices, including network device discovery and maintenance, route configuration, interface management, Layer-2 link management, IP topology, device accessories, and AR voice management. |
| eSight PON Manager | Manages and monitors Huawei passive optical network (PON) devices in a unified manner. |
| eSight Server Device Manager | Manages and monitors Huawei servers in a unified manner by offering an impressive array of functions, including centralized fault monitoring, performance analysis and report, keyboard, video, and mouse (KVM), and integrated virtual media management. |
| eSight Host Manager | Monitors the host operating system, including the CPU, memory, disk, and network adapter. Mainstream operating systems, including Windows, Red Hat, and SUSE, are supported.  note  The host agent must be installed on managed hosts. |
| eSight Virtualization Manager | Manages virtual resources in a unified manner, including virtual resource discovery and monitoring. |
| eSight Storage Device Manager | Offers unified management over storage devices of different types and from different vendors, including storage device discovery, maintenance, and query. |
| eSight UC Device Manager | Offers convenient and quick UC device configuration, wizard-based service installation and configuration, one-stop service rollout, end-to-end visual network surveillance, and intuitive display of fault information, helping users quickly locate and rectify problems. |
| eSight Intelligent Video Surveillance Device Manager | Offers end-to-end management over video surveillance devices, including resource discovery, topology, performance, and data analysis, which effectively improves video surveillance device management quality and efficiency. Users can view the performance and alarm data about surveillance devices to learn about the device running status and quickly locate faults. |
| eSight Telepresence and Video Conference Device Manager | Supports the access of servers and endpoints to the telepresence conference, alarming, and topology management, monitors the network of telepresence conference sites, and provides assurance for the network of critical conferences. It can enhance O&M personnel's awareness of the network quality at telepresence conference sites, enabling them to locate network faults efficiently. |
| eSight eLTE Device Manager | Manages Huawei's enterprise Long Term Evolution (eLTE) devices, including plug and play (PnP), device firmware upgrade, device configuration management, and remote device maintenance. |
| eIMS Device Manager | Manages NEs of eIMS devices and ensures the effective network O&M in scenarios including site deployment, service configuration adjustment, and daily maintenance. |
| eSight Application Manager | Monitors the following items in real time: mainstream operating systems, databases, email servers (such as Exchange), middleware (such as IBM MQ, MSMQ, and Sharepoint), application servers (such as Tomcat, WebLogic, JBoss, GlassFish, and Microsoft .Net), and services (such as AD, DNS, FTP, and LDAP). This function keeps users abreast of the application status and ensures the normal operation of applications. |
| Service management components | eSight Open SDK | Provides SNMP and HTTP interfaces to be integrated by third-party systems. |
| eSight Smart Reporter | Pre-integrates rich report templates, meets network O&M report requirements, and allows users to customize report templates. |
| eSight Reporter | Enables users to quickly and flexibly customize reports by drag and drop and displays the reports graphically. |
| eSight Network Report Template Package | Provides indicator analysis reports of the NE, board, port, link, radio frequency, AP, and SSID, including indicator statistics, indicator change trend, reports on Top N indicators, and custom reports. |
| eSight WLAN Manager | Manages wireless network resources (AC/AP), diagnoses wireless network faults, and displays wired and wireless devices in the topology. |
| eSight MPLS VPN Manager | Automatically discovers MPLS VPN services, presents the logical architecture of the VPN network, and monitors and collects statistical information about the VPN service status and quality. |
| eSight MPLS Tunnel Manager | Automatically discovers deployed MPLS TE and LDP tunnels, dynamically presents the network channel status change, and enables visual route management. |
| eSight Network SLA Manager | Automatically performs periodical and temporary diagnosis over network lines, which helps users to assess network service quality. |
| eSight Network Traffic Analyzer Manager | Analyzes network traffic packets based on the packet source, destination, protocol, and application, which helps users to understand network traffic distribution. |
| eSight IPSec VPN Manager | Manages IPSec VPN services on the GUI as follows: discovers IPSec VPN services, displays IPSec VPN services in the topology, and supports VPN tunnel information query. |
| eSight Secure Center | Centrally manages policies for Huawei network security devices, including firewall, intrusion prevention system (IPS), and antivirus policies. |
| eSight Server Stateless Computing Manager | Virtualizes server hardware to configure and manage stateless Huawei servers through configuration files. |
| eSight Server Deployment Manager | Configures Huawei servers in batches, including BIOS configuration, network configuration, RAID card configuration, and operating system deployment. |
| eSight Storage Report Template Package | Provides analysis reports for performance and capacity, including resource statistics, capacity trend, Top N capacity reports, Top N performance reports, and custom reports. |
| eSight SAN Analyzer | Monitors and analyzes SAN/NAS storage network environments, automatically discovers storage network topologies, centrally monitors storage network alarms, and monitors and compares storage link performance.  Supports two monitoring views (global and custom topologies) and displays storage resources, storage mappings, host paths, and host logical relationships in drill-down mode, facilitating multi-level monitoring and analysis over storage paths. |
| eSight Capacity Manager | Summarizes and analyzes capacity information about hosts, virtual machines, and virtual servers, including capacity usage statistics, hot spot distribution, and trend prediction. With capacity management, eSight predicts the capacity usage trend within one week, two weeks, three weeks, and one month, instructing users to perform capacity expansion. |
| eSight Data Center Manager | Monitors virtual computing resources of data centers in each region and end-to-end services in each application system. |
| eSight Facilities Infrastructure Manager | Manages basic facilities in an equipment room, including power supply, cooling, access control, physical security, environment, firefighting, and lighting devices, as well as cabinets and collectors. Offers enhanced energy efficiency analysis, temperature nephogram, and capacity management functions. |

1. Lightweight System to Easily Access the Network and Keep Abreast of the Network Status

Based the browser/server (C/S) architecture, eSight is free of client installation. During system upgrade or maintenance, the software on the server side is updated, reducing upgrade or maintenance costs. The advantages are as follows:

* Allows users to perform operations such as querying and browsing anywhere at any time based on the distributed feature.
* Allows users to expand services only by upgrading the server software.

1. Unified Vendor and Resource Management to Unify Network Management

eSight offers holistic device management capabilities. eSight allows users to:

Manage Huawei routers, switches, ARs, security devices, WLANs, firewalls, UC devices, and storage devices.

Predefine management capabilities over devices from mainstream vendors, including HP, Cisco, and H3C. Users can customize the device vendor, type, performance, and alarm management.

Default adaptation plan for vendors

eSight provides basic adaptation capabilities for devices from Huawei, Cisco, and H3C, including topology management, standard alarms, standard performance counters (CPU/memory), configuration file backup, and panel display.

User-defined device management plan

eSight supports customization of basic management functions for unknown devices by entering the device object identifier (OID), alarm information, performance counters, configuration commands, and high-fidelity panels.

1. Independently Deliverable Device Adaptation Package

eSight uses the component-based design to make connections between devices and services logically independent, which speeds up the software development in support of new device types without influencing the entire system architecture or stability. To adapt to new devices, customers only need to upgrade adaptation packages of some devices, which avoids a comprehensive upgrade that may take a long time and cause service interruption.

1. Openness and Integration

eSight offers diverse open interfaces to be integrated into customers' service processed by third-party vendors.

eSight provides the following interfaces:

* HTTP/HTTPS-compliant Restful interfaces: Use the standard Rest style to offer interfaces for querying managed resources and alarms as well as acknowledging and clearing alarms.
* SNMP-compliant interfaces: Offer interfaces for obtaining managed resources as well as acknowledging and clearing alarms, and report data change to collecting parties in the form of notifications.

1. Hierarchical Network Management

eSight supports hierarchical network management. The upper-layer NMS can monitor and maintain the lower-layer NMS in a unified manner. An upper-layer NMS can manage up to 500 lower-layer systems in a centralized manner. After a lower-layer NMS is added to an upper-layer NMS, the eSight system automatically synchronizes resources from the lower-layer NMS to the upper-layer NMS. The upper-layer NMS can centrally manage all its lower-layer NMSs through its capabilities, including unified management over topologies, resources, alarms, user authentication, and portlet summary. Users can directly jump to a lower-layer NMS from the upper-layer NMS for further operations over a specific managed object.

## Unified Monitoring, Diagnosis, and Troubleshooting

The primary task of operation and maintenance is to monitor the running status of ICT environments in real time, quickly locate and troubleshoot faults, and effectively prevent potential risks.

eSight offers a complete set of monitoring, analysis, and troubleshooting functions to help users detect and rectify faults in a timely manner and ensure the normal operation of enterprise ICT environments. The following table lists the management functions.

|  |  |
| --- | --- |
| Function | Description |
| Performance management | Supports performance data collection, report analysis, and Portal top N monitoring, which monitor, analyze, and evaluate networks and devices. |
| Fault management | Receives traps reported by devices, pushes the traps and topologies to the web page, and notifies users of network faults by short messages or emails in a timely manner. |
| Network fault diagnosis (telepresence conference) | Collects and displays network performance indicators on devices that media streams pass through, visually presents the running status of the network, and facilitates decision making for network deployment and service adjustment. |
| Configuration management | Backs up device configuration files and restores the configuration using the backup configuration files when a device fault occurs or components on a device are replaced. |

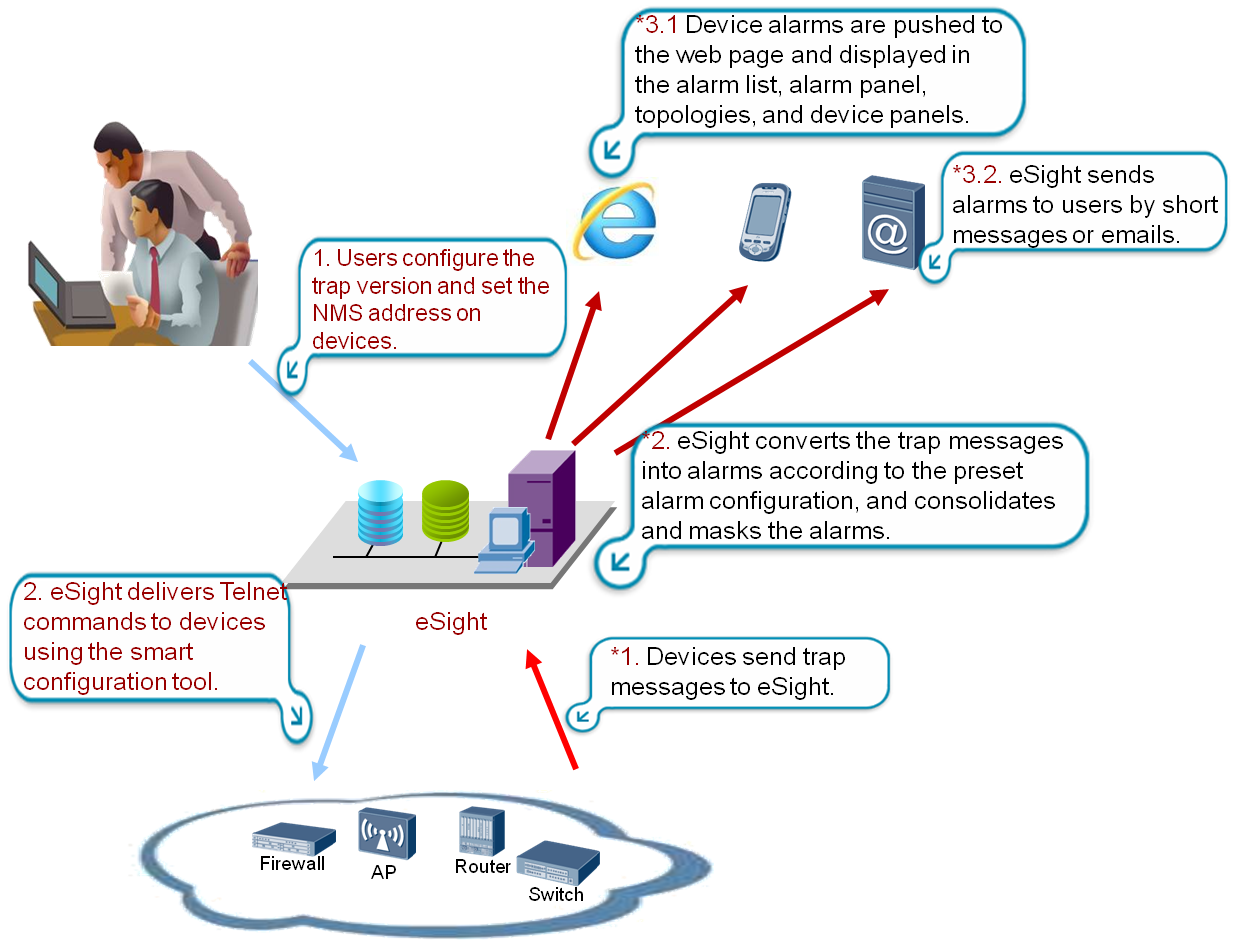
### Performance Collection and Prediction Analysis

#### Introduction

By collecting and displaying various performance data of devices, eSight enables users to learn about the network health conditions and make correct decisions about network deployment and service adjustment.

In addition, eSight provides the report analysis and Top N data display functions, enabling enterprise network management administrators to learn about the ICT system running status.

Performance management solution



eSight also provides an NTA component to allow users to analyze service flows based on parameters such as protocols used on networks.

#### Key Technologies

1. Performance Collection Task Management

Based on created performance tasks, eSight collects performance indicator data at specified intervals when devices and service applications are running in ICT systems.

1. Performance Data Consolidation

eSight collects device performance data at regular intervals and stores the data in the database. By default, eSight stores the original performance data within the latest three months and stores only the summarized data when three months are exceeded. Performance data is summarized by hour and day. By default, hour-based data is stored for one year and day-based data is stored permanently until deleted by users. Users can perform summary statistics and trend analysis based on stored data.

#### Function Constraints

1. Applicable Device Type Constraint

Preset alarm adaptation information varies according to device types. For details, see the *eSight Device Specification List.*

1. Technical Constraint

The protocol parameters such as **SNMP** must be correctly configured.

#### Typical Applications

* Scenario 1: Keep an eye on the health of key indicators and detect potential risks.
* Users can set performance indicators to concern and set thresholds. When the thresholds are reached, eSight sends alarm notifications to notify specified management personnel.
* Scenario 2: Collect the overall system running status, learn about the trend, and make plans.

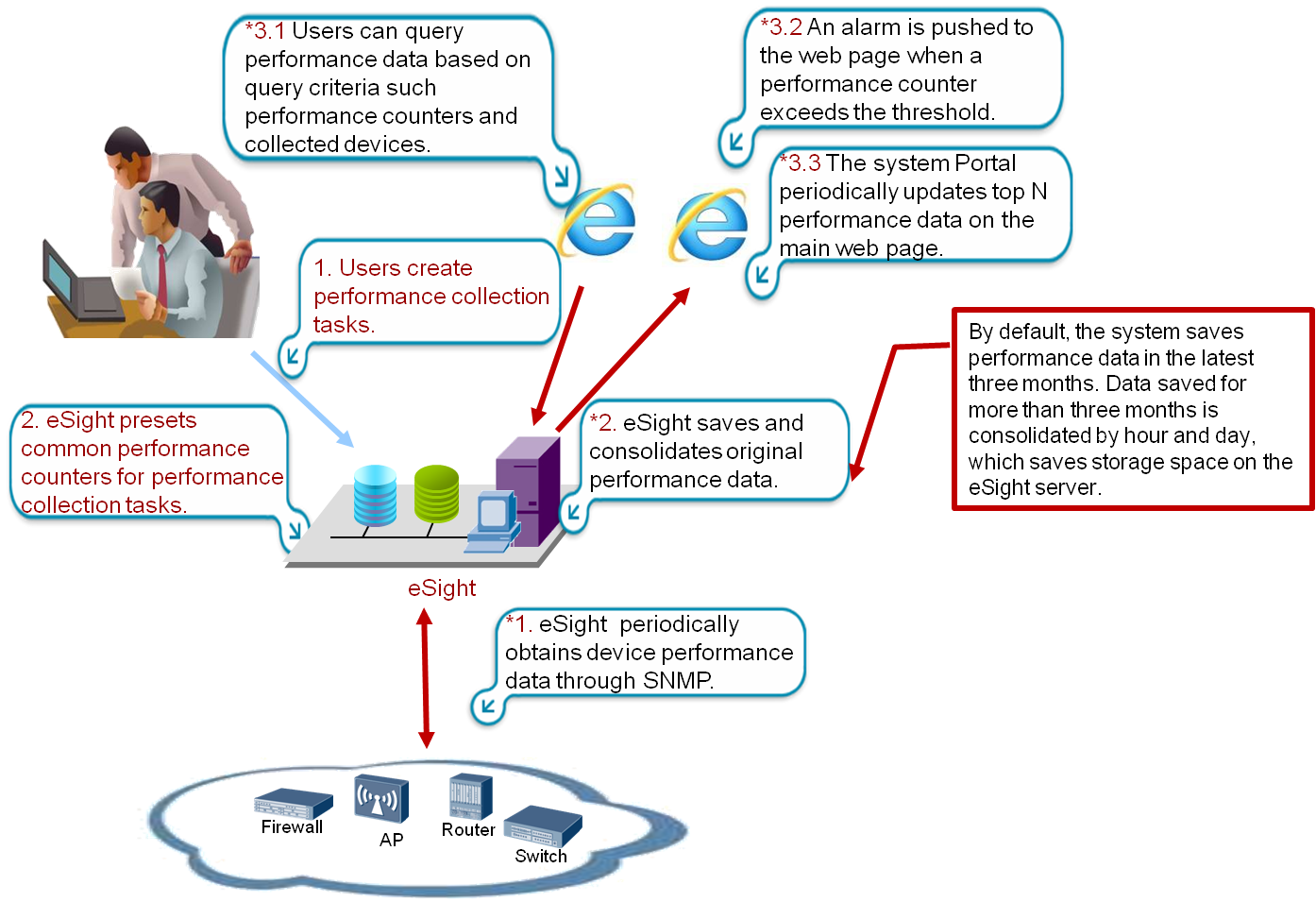
Users configure performance statistics report templates and the time to send. eSight collects and analyzes the system running status at regular intervals and automatically sends the data to specified email addresses, which significantly saves time and labor costs.

### Alarm Information Collection and Notification

#### Introduction

When a device or application fault occurs, eSight can collect all the possible fault information in time, generate an alarm accordingly, and notify the maintenance personnel of the fault by means of SMS or email in time.

Alarm management solution



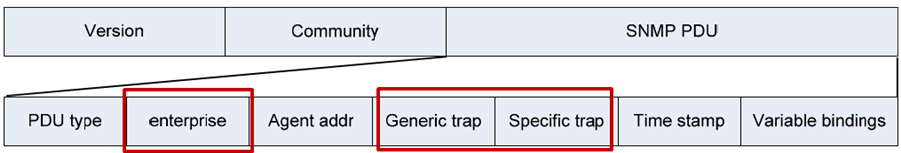
If notifications (such as SNMP trap messages) are sent to eSight due to device faults, eSight automatically parses these notifications as alarms based on preset parsing rules, and notifies users of the alarms by displaying the alarms on the GUI, sending SMS messages, or sending emails.

#### Key Technologies

1. Trap Receiving

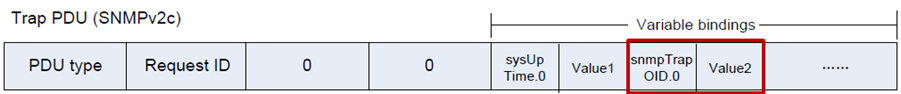
Network devices usually report alarms to eSight through SNMP trap messages. Devices can send SNMP trap messages to the destination address specified using commands. eSight supports trap messages of SNMPv1, SNMPv2c, and SNMPv3.

* SNMPv1 trap message



The fields **enterprise** (trap source type), **Generic Trap** (common trap), and **Specific trap** (enterprise private trap) uniquely identify a trap message. eSight parses the **Variable bindings** field in the trap message and displays the parsed value on the web page.

* SNMPv2c and SNMPv3 trap messages



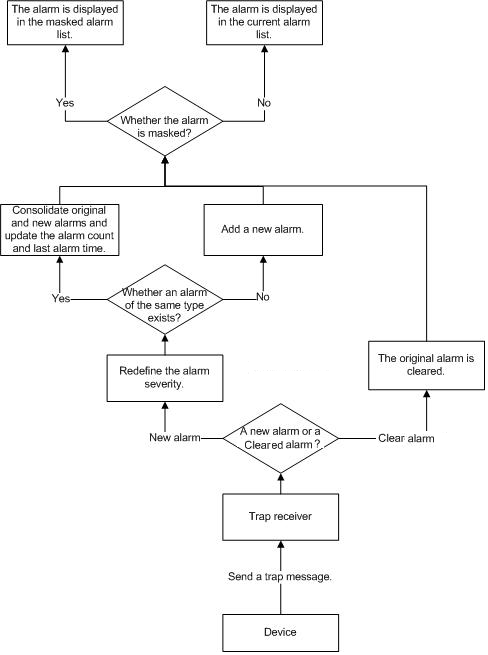
The field **snmpTrapOID** uniquely identifies a trap message. eSight parses the **Variable bindings** field in the trap message and displays the parsed value on the web page.

Compared with the SNMPv2c trap message, an encryption header is added to the SNMPv3 trap message. The packet data unit (PDU) is the same in the SNMPv2c and SNMPv3 trap messages.

1. Alarm Handling Principle

After receiving trap messages, eSight parses the trap messages based on the static alarm configuration, redefines the alarm severity, and masks alarms.

The following uses the SNMP trap message as an example.



1. Compliance with Multiple Protocols

In addition to SNMP, eSight also supports TR069 and MML alarm messages.

#### Function Constraints

1. Applicable Device Types

Preset alarm adaptation information varies according to device types. For details, see the *eSight Specification List.*

1. Technical Constraint

The relevant protocol parameters (such as **SNMP read community**) must be configured correctly on both the device and the network management server.

#### Typical Applications

* Scenario 1: Obtain the alarm status about devices on the eSight client in real time.

When a new alarm arrives, eSight notifies users of the alarm by blinking the alarm panel, displaying numbers on the alarm panel, generating alarm sounds, and refreshing the alarm browsing page. When viewing the device panel on the topology management page, users can also find alarm devices that are identified by different colors, which allows users to learn about the health conditions of devices when performing other operations.

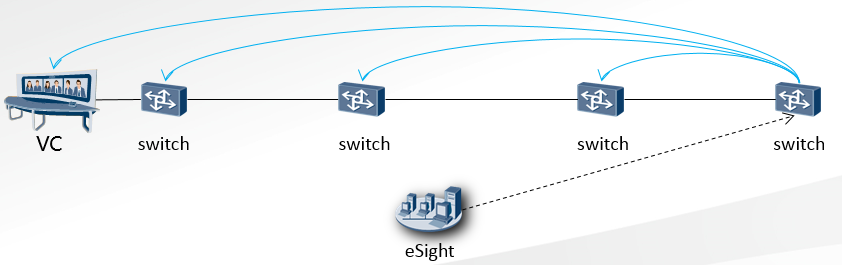
* Scenario 2: Obtain alarm notification even when users do not log in to the eSight client.

After users set the phone number and email address for alarm forwarding and their concerned alarm severity in the eSight system, eSight notifies users of specified alarms using specified methods.

### Network Fault Diagnosis (Telepresence Conference)

#### Introduction

eSight can monitor the network periodically using the SLA diagnosis function before and in a telepresence conference. When eSight discovers network abnormalities, it will automatically check the network quality segment by segment to ensure network stability. eSight mainly monitors the packet loss rate, jitter, and delay. Based on the data of telepresence conferences and media streams, eSight monitors the performance indicators of network devices which are in the network route and displays the monitoring data.



#### Key Technologies

1. Site Monitoring

According to the network links of each site that have been defined by O&M personnel, eSight automatically and periodically inspects the running status of devices on the links and network quality. When problems appear, eSight will automatically diagnose the faults and generate alarms. It can also export the long-term monitoring data for review.

1. Conference Assurance

eSight allows O&M personnel to closely monitor the network quality of each conference site and discover abnormalities during a telepresence conference. It can also store the network quality data for later analysis and review.

#### Function Constraints

1. Applicable Device Types

Network devices need to support the NQA capability. If devices on a link do not support NQA or diagnosis is not appropriate in certain scenarios, you shall not specify the devices as diagnosed devices when specifying the link.

1. Technical Constraints

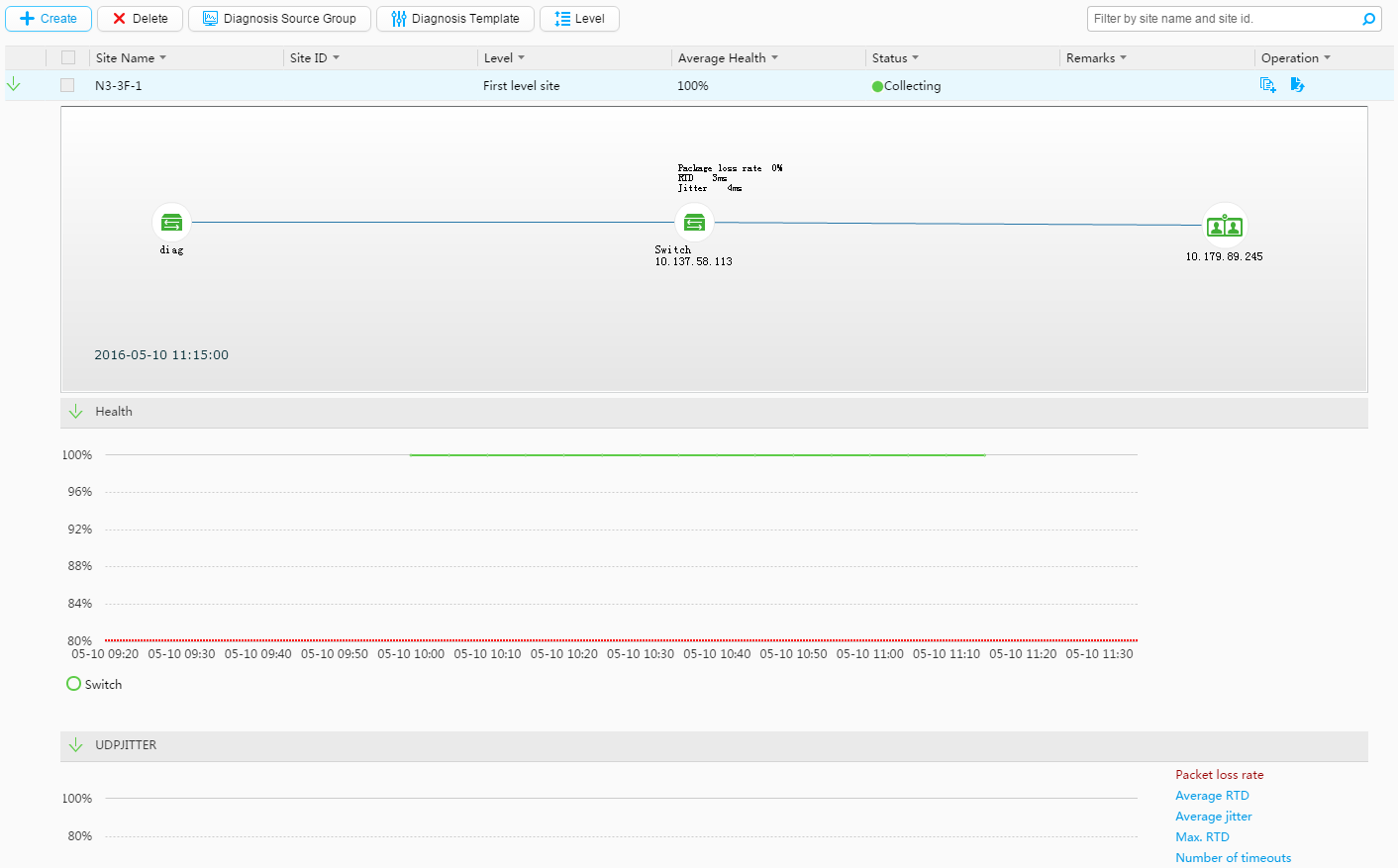
None

#### Typical Applications

Scenario 1: routine conference network monitoring

In the eSight system, users can check the conference topology. Network quality monitoring is performed at regular intervals.

Conference maintenance and routine monitoring



The figure above is the conference maintenance page where you can add conference sites, configure diagnosis devices, and set diagnosis parameters.

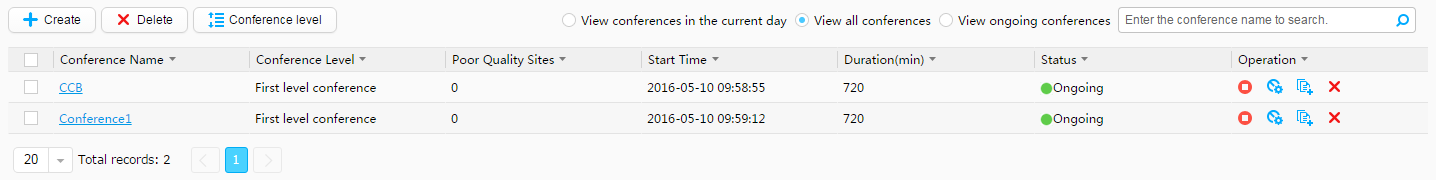
Presentation services in the graphical zone have the following features:

* Display conference information and network health in a list.
* Expand the list to view the topology of each conference site, and check network quality between diagnosed devices and diagnosis devices.
* View the network health trend diagram and health indicator trend diagram under the topology.

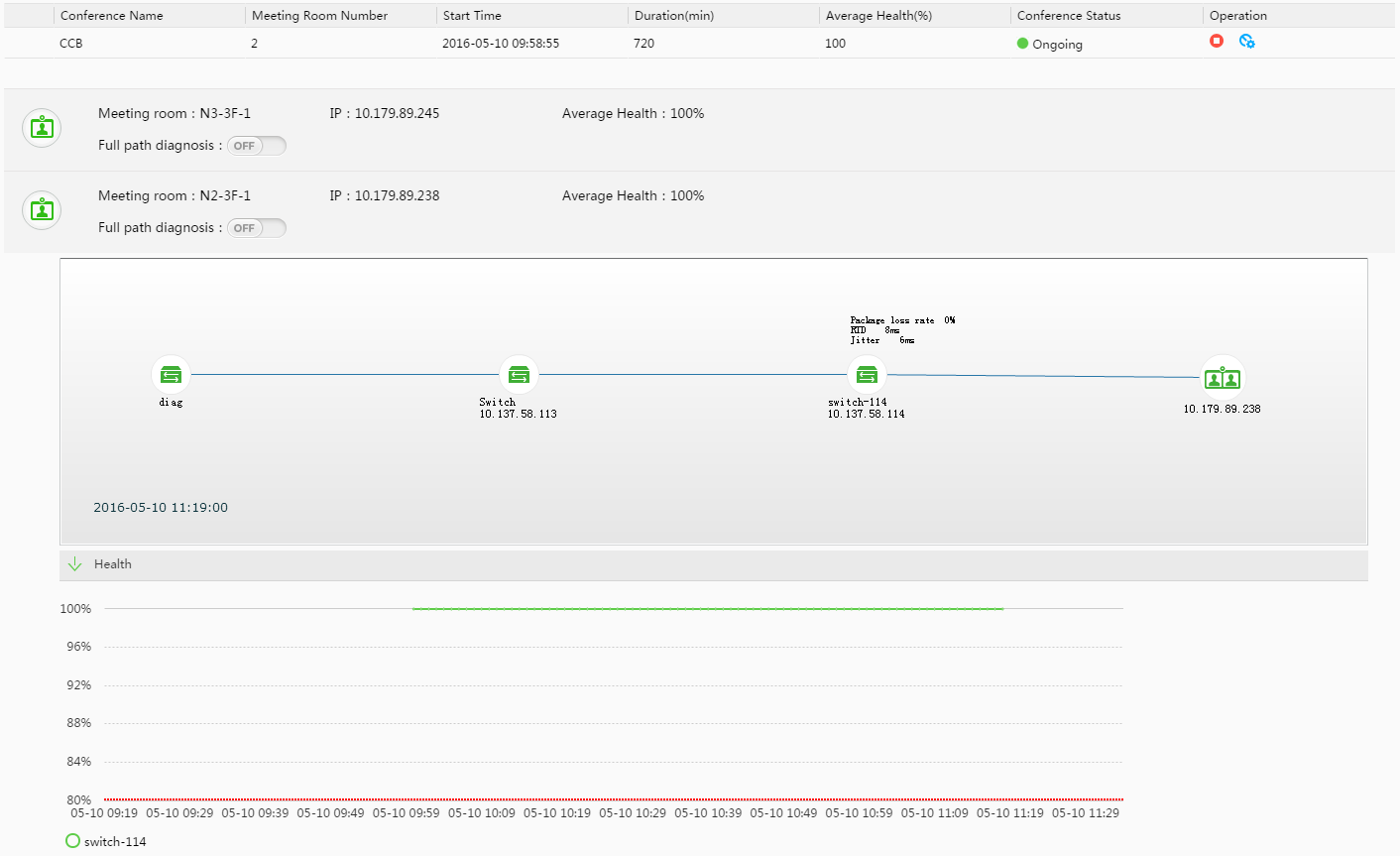
Scenario 2: support for important conferences

In the eSight system, users can schedule conference support tasks.

Conference support task scheduling and conference list



Support for important conferences



During conference diagnosis, O&M personnel can use eSight to monitor the network status of each conference site in real time. The system marks any conference site in red if its network status is lower than the specified threshold. Users can expand the conference site list to view the network health status and indicator trend diagrams during the conference.

Presentation services in the graphical zone have the following features:

* Display the conference topology and display abnormal devices in colors.
* View network quality of each device in the topology link and detailed quality information.

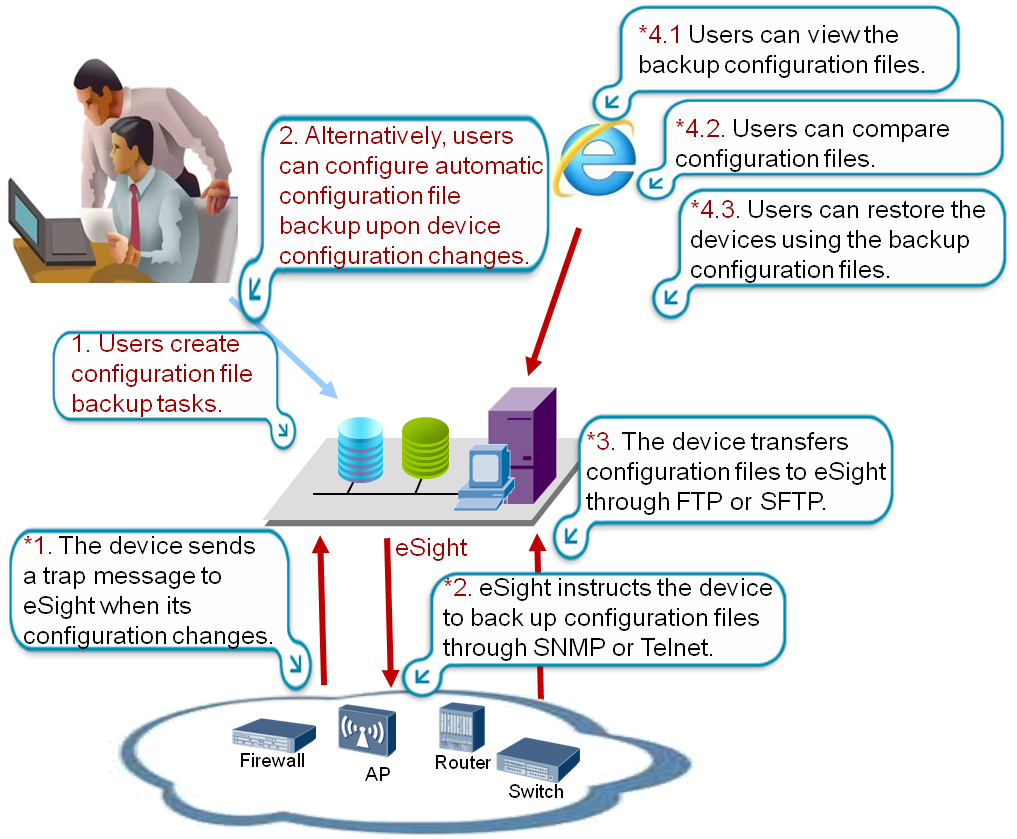
Diagnosis data will be saved after a conference ends. Users can query and export historical conference data.

### Rapid Configuration Backup and Restoration

#### Introduction

Services cannot run properly if the parameter settings are incorrect. When a device is replaced or services are adjusted, the relevant parameters must be reconfigured. Such reconfiguration, which usually involves a large number of parameters, is complicated, time-consuming, and error-prone. eSight provides the configuration backup and management function. Users can back up the configurations of important devices and quickly restore normal network operations using the backup data when a device is faulty or replaced.

Configuration file backup



#### Key Technologies

eSight can function as a File Transfer Protocol (FTP) server or a Secure File Transfer Protocol (SFTP) server. eSight instructs devices to back up configuration files using the MIB interface or command lines periodically, or when the device configuration changes. Devices upload configuration files to the specified directory on eSight using FTP or SFTP.

* Scheduled backup

eSight instructs devices to back up and restore data through preset protocol interfaces at scheduled intervals specified in tasks.

eSight instruct devices to back up and restore data through the command-line interface.

* Change-based backup

When the configuration of a Huawei device changes, it sends a trap message to eSight. After receiving the trap message, eSight notifies the Huawei device of configuration file backup and restoration through Huawei proprietary MIB interface.

#### Function Constraints

1. Applicable Device Types

By default, the configuration file backup function has been configured for Huawei, Cisco, and H3C devices. Users can set command lines for backing up configuration files of devices from other vendors.

1. Technical Constraint

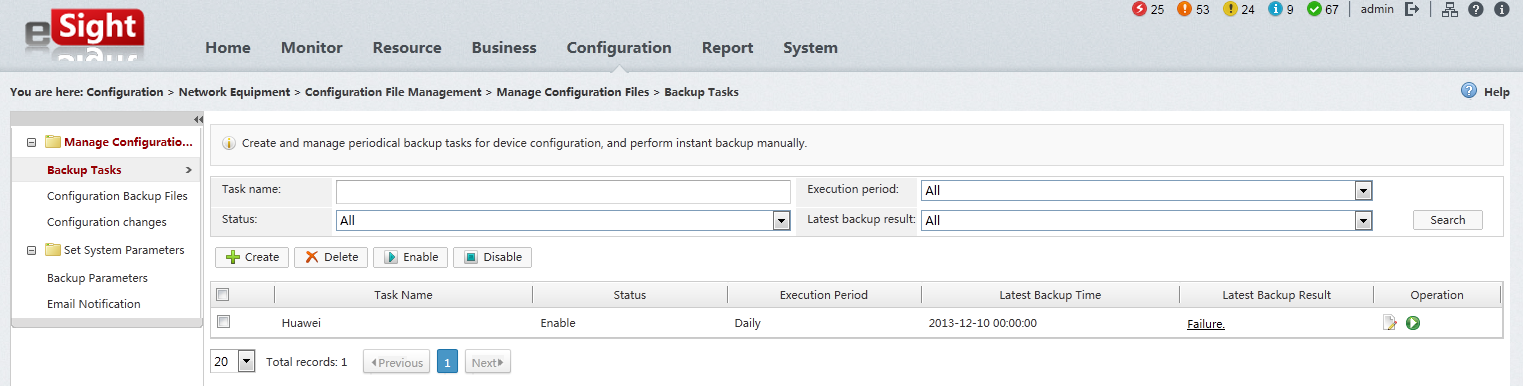
The parameter **SNMP Read** and **SNMP Write** must be correctly set on Huawei devices and eSight. Command lines and Telnet parameters must be set on third-party devices and eSight.

#### Typical Applications

Scenario: In case of a device fault, eSight determines whether it is because of configuration and quickly clears the fault through backup data.

eSight backs up configuration data based on preset rules. In case of a network fault, eSight compares the current configuration file with the baseline file. If detecting any difference, eSight restores the backup configuration file on devices to restore configuration and clear the fault.

Backup task



## Security Management

eSight is the direct controller of the entire ICT environment. If eSight is attacked by viruses or improper operations are performed by unauthorized personnel due to incorrect rights control, exceptions may occur on eSight and the entire ICT environment as well, which may even cause system breakdown and cause huge losses. Therefore, the security management capability of eSight is essential.

eSight security solution ensures eSight software security. In addition, eSight provides suggestions on the security of the physical layer and management layer to ensure the implementation of security measures. The security solution covers the following three aspects:

* Application layer security: protects applications with a variety of security measures such as access control, data security, and communication and coding security.
* System layer security: protects operating systems, databases, middleware, and services that applications depend on.
* Network layer security: protects the entire network to ensure that all service systems running on the network are stable.

For details, see the *eSight Security Technology White Paper*.

# Conclusion

eSight offers a comprehensive lineup of monitoring and location approaches, supports the access of diverse devices, and monitors IP networks as well as storage, UC, telepresence, and video surveillance devices, which helps users learn about the network and service quality in real time.

eSight uses the component-based architecture to offer an impressive array of service components for users to build their own ICT management system based on the flexible combination of service components, which reduces user investments while ensuring the network security.

# Acronyms and Abbreviations

|  |  |
| --- | --- |
| **F** |  |
| FTP | File Transfer Protocol |
|  |  |
| **I** |  |
| ICT | Information and Communications Technology |
|  |  |
| **M** |  |
| MCU | Multipoint Control Unit |
| MIB | Management Information Base |
| MML | Man-Machine Language |
|  |  |
| **O** |  |
| OSS | Operating Support System |
|  |  |
| **R** |  |
| RSA | Revist-Shamir-Adleman Algorithm |
|  |  |
| **S** |  |
| SFTP | Secure File Transfer Protocol |
| SLA | Service Level Agreement |
| SMC | Service Management Console |
| SNMP | Simple Network Management Protocol |